October 14, 2003

10

Public Information Room
Office of the Comptroller of the Currency
250 E Street, S.W., Mail stop 1-5
Washington, D.C. 20219
Attention: Docket No. 03-18

Regulation Comments
Chief Counsel's Office
Office of Thrift Supervision
1700 G Street, N.W.
Washington, D.C. 20552
Attention Docket No. 03-35

Ms. Jennifer J. Johnson
Secretary
Board of Governors of the
Federal Reserve System
20th Street and Constitution Ave., N.W.
Washington, D.C. 20551
Docket No. OP-1155

Robert E. Feldman
Executive Secretary
Attention: Comments/OES
Federal Deposit Insurance
Corporation
550 17th Street, N.W.
Washington, D.C. 20429

Re: Proposed Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice

Dear Sirs and Madams:

This comment letter is submitted to the Board of Governors of the Federal Reserve System (the "Board"), the Federal Deposit Insurance Corporation ("FDIC"), the Office of the Comptroller of the Currency ("OCC"), and the Office of Thrift Supervision ("OTS") (collectively, the "Agencies") on behalf of Wachovia Corporation, Wachovia Bank, N.A. and their subsidiary companies (collectively referred to as "Wachovia"). Wachovia is pleased to provide comments on the proposed Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice issued on August 12, 2003 ("Interagency Guidance").

Wachovia recognizes the difficult regulatory challenge presented in crafting guidelines for response programs for unauthorized access to customer information and applauds the work of the Agencies in addressing this issue. We also commend the Agencies for their efforts to ensure that Gramm-Leach-Bliley creates benefits in the marketplace and adequately safeguards customer information. Finally, we hope that these comments will be helpful to the Agencies in developing the final Interagency Guidance.

Generally, Wachovia believes that there is no need for additional regulation in the area of customer notification. Section 501(b) of the Gramm-Leach-Bliley Act already provides standards to safeguard customer information. In addition, if the proposed Interagency

Guidance is a response to identity theft and fraud issues in the marketplace, the financial services industry has already taken the initiative by encouraging financial institutions to create their own comprehensive response programs to secure customer information.

Standard for Providing Notice

Generally, Wachovia agrees with the approach of the Interagency Guidance not to require notification to potentially affected customers in each case that unauthorized access to sensitive customer information may have occurred. However, Wachovia believes the Interagency Guidance should place greater reliance than currently proposed on a risk-based approach to customer notification.

The Interagency Guidance is too prescriptive in imposing requirements for financial institution response programs. Most instances of unauthorized access to customer information do not lead to misuse, and it is not necessary to mandate customer notification in each of these situations. Formulaic approaches to customer notification like California's SB 1386 can mandate customer notification in situations that would not provide any benefit to the customer, and excuse notification in situations in which communication about the event to the customer would be valuable.

Wachovia favors standards that would require each financial institution to establish a flexible program that (i) considers the risks to customer information in the event of unauthorized access to the information and (ii) provides a response that matches the risk and probable impact on the customer. Regardless of whether or not notice to customers is deemed appropriate, the financial institution should take reasonable steps to protect the affected customers from harm such as monitoring potentially affected accounts. This would allow the financial institution to match its response to the threat. Wachovia believes that many responsible financial institutions currently handle security incidents in this manner.

Interagency Guidance Should Serve as the National Standard

Wachovia recommends that the Agencies take steps to provide that the Interagency Guidance expressly preempt inconsistent state law where such state law does not afford any person additional protection above what is already provided under the Gramm-Leach-Bliley Act. As discussed above, California has adopted SB 1386 which mandates notice of certain unauthorized access to customer information regardless of the potential for misuse of the information. As a result, in many circumstances SB 1386 does not provide additional protection to its residents above what is provided under the Interagency Guidance. Even if the potential for misuse is remote, California SB 1386 forces notification of individuals that can be unnecessarily alarming, and if the notifications become frequent enough, could be routinely ignored.

Financial institutions that provide a mandated notice to California customers would be driven by customer expectations to provide notice to similarly situated customers who reside in other states. As a result, the California statute would become the de facto

national standard without providing individuals meaningful benefits that support the goal of reducing identity theft. In the absence of preemption, the California statute would have the effect of diluting the impact of notifications provided under the Interagency Guidance. Therefore, Wachovia recommends that the Interagency Guidance preempt inconsistent state and local laws.

Allow Delay of Notification to Protect an Investigation

In certain cases, notification should be delayed to avoid compromising the investigation of the event. Publicity may confirm for a culprit the significance of access to certain information, or may notify the culprit that access has been discovered and inhibit efforts to apprehend the individual. Therefore, the Interagency Guidance should allow financial institutions to consider delaying notification to customers if the financial institution determines that notice would impede investigation of the event and would further subject information to misuse. To provide appropriate flexibility, the Interagency Guidance should not require a determination by law enforcement officials, as is currently required under California law, that notification should be delayed.

The Definition of Sensitive Customer Information Should be Consistent with Potential Risks from Misuse

In order to appropriately balance protecting customer information and facilitating customer transactions, financial institutions utilize risk-based controls to access information and to engage in transactions. Similarly, the definition of sensitive customer information should be consistent with the information that may be required to engage in sensitive transactions. Financial institutions typically require account numbers to be accompanied by customer access numbers, personal identification numbers or code words to complete sensitive transactions like electronic bill payment, or account and customer record changes. The definition of "sensitive customer information" should reflect this risk-based authentication process. Wachovia recommends that "sensitive customer information" be defined as an individual's last name and first name or first initial in combination with any of the following data elements: (1) social security number, (2) driver's license number or other government issued identification card, or (3) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

In addition, encrypted information should not be considered sensitive customer information unless there was reason to believe the encryption had been or could be broken by processes easily accessible in the marketplace. Not including encrypted data in the definition of sensitive customer information may motivate companies to continue efforts to encrypt sensitive data. Similarly, if customer information is protected by robust passwords even though a computer or other access device has been lost or stolen, the financial institution should be allowed to conclude that the customer information has not been accessed. Financial institutions should consider whether or not the data is encrypted or otherwise protected when conducting their risk-based analysis of whether or not the customer will be harmed.

Publicly available information, defined as information that is lawfully made available to the general public from federal, state, or local government records, should also be excluded from the definition of sensitive customer information.

Notification to Regulators Should Occur Only When the Incident Presents Significant Risk of Substantial Harm to a Significant Number of Customers

As currently drafted, Section II.B places a heavy burden on a financial institution to notify its primary regulator whenever it learns of any incident involving unauthorized access that could result in substantial harm or inconvenience to its customers. This standard could require notification of virtually every incident where substantial harm is "possible" no matter how unlikely. This standard should be modified to be consistent with the risk-based approach to notice that Wachovia supports. Financial institutions should inform regulators about significant incidents. Accordingly, notification under Section II.B should be expected when an incident poses a significant risk of substantial harm to a significant number of customers.

Modifications to Examples of When Notice Is /Is Not Expected

Wachovia recommends that, the following modifications be made to the first and last examples described in the Interagency Guidance of situations where notice would not be expected. The first example, where an institution can retrieve sensitive customer information that was stolen, should be expanded to exclude both retrieving or destroying the information. In addition, the last example, concerning theft of a laptop, should be expanded to provide that notice is not expected if the data was encrypted or if the data is protected from access by a secure token or other similarly secure access device. These modifications would reflect the low risk of harm to the customer.

The first and third examples described in the Interagency Guidance where notice would be expected to be given should also be modified. The first example, concerning an employee obtaining unauthorized access to sensitive customer information, should include as an additional element a likelihood of misuse of the information to the detriment of the customer. In addition, the third example involving a loss or theft of electronic media, should be limited to situations in which the electronic media is not protected by passwords, encryption or other security devices. These modifications would reflect the likelihood of misuse and resulting harm to the customer.

Corrective Measures Requirements

The Interagency Guidance directs financial institutions to take enumerated steps (i.e., flag accounts, secure accounts, customer notice and assistance) in the event of unauthorized access to sensitive customer information. The response of the financial institution should match the threat and each item may not be appropriate for each situation. Therefore, the Interagency Guidance should direct the financial institution to consider taking the enumerated steps.

Secure Accounts

The expectations in the Interagency Guidance associated with securing an account are not clear. Regardless of how "secure the account" is defined, the requirements of the section are too prescriptive. Since appropriate actions to secure an account will depend on the specific situation, the Interagency Guidance should generally describe actions the financial institution should consider to mitigate the risk to the account such as monitoring the exposed accounts or changing account numbers. The requirement for customer assent to the actions of the financial institution is overly broad and should be eliminated. This requirement would be operationally impractical in any situation that involved more than a few customers, and does not take into account that the financial institution may have taken actions for which customer consent is unnecessary.

Manner of Delivery of Notice

The Interagency Guidance should provide flexibility in the delivery of notice to allow a financial institution to determine the type and manner of notice that may be appropriate. In certain narrow, high-risk situations, the financial institution should attempt to notify affected customers by telephone, and in other low risk situations, notice by mail may be appropriate. For example, in certain wide ranging security compromises, such as those involving VISA processors, individual notice may not have been appropriate because of the high cost, the low probability of harm, and the limited benefit to consumers. The guidance on notice should allow financial institutions to consider notice through the media, through websites, or only in response to inquiries as it deems appropriate.

The proposed Interagency Guidance states in Section 3.a. that "customer notice should be timely, clear, and conspicuous, and delivered in any manner that will ensure that the customer is likely to receive it." It is difficult to ensure that a customer will receive a communication. Instead, a financial institution should be encouraged to deliver notice in a manner appropriate for the circumstances and utilizing the most recent contact information currently available to the institution.

Content of Customer Notice

Although all of the recommended notice elements might be appropriate in a specific situation, each element may not be appropriate in a given circumstance. Since a response may not be necessary in a given circumstance, the notice elements should be considered by the financial institution for inclusion in a notice but the elements contained in a notice should not be mandatory. For example, a financial institution may notify customers of a compromise of their information but reasonably conclude that the risk of misuse is slight. In that situation, it may not be appropriate to recommend that a fraud alert be placed in the customer's credit file because of the low risk of harm and the negative impact the fraud alert could have on the customer being able to receive credit approval in a timely manner.

The recommendation that customers remain vigilant "over the next twelve to twenty-four months" may not be appropriate to the specific fact situation. Instead, the Interagency Guidance should only state that customers should remain vigilant.

Conclusion

Wachovia appreciates the opportunity to comment on this proposal. Should you wish to discuss any elements of this letter further, feel free to contact Jeff Glaser, Vice President and Assistant General Counsel (704) 374-4642, or me at (704) 374-4645, at your convenience.

Very truly yours,

Campbell Tucker
Director, Privacy Office

cc: via electronic mail
Wachovia Corporation:
Mark Treanor, Senior Executive Vice President and General Counsel
Michael Watkins, Senior Vice President and Deputy General Counsel